Feuille TD - Chiffrement symétrique

Exercice 1 (Preuve de la perfection du code de Vernam)

1. *Démontrer que pour un code secret où la clef K est générée aléatoirement pour chaque message M on a $H(M|K) = H(M)$.*
2. *En utilisant les entropies conditionnelles et la définition du code de Vernam, démontrer que dans un code de Vernam ($C = M \oplus K$), on a toujours $H(M,K,C) = H(M,C) = H(M,K) = H(C,K)$; en déduire des relations entre les entropies conditionnelles de M, C et K.*
3. *Démontrer que le chiffrement à clef jetable de Vernam est un chiffrement parfait.*

Exercice 2 (Chiffrement affine) *Un chiifrement affine, dont le chiffre de César est un cas particulier, est défini comme suit. Soit p un nombre premier et soient a, b deux entiers non nuls choisis dans $\{1, \ldots, p-1\}$. On note $\Phi_{a,b,p}$ la fonction de $\mathbb{Z}/p\mathbb{Z}$: $\Phi_{a,b,p}(x) = (a.x + b) \mod p$.*
Pour un message dans $\{0, \ldots, p-1\}$, on considère la fonction de codage $E = \Phi_{a,b,p}$.

1. *Expliciter la fonction de décodage D associée à E en montrant qu'elle s'écrit sous la forme $D = \Phi_{\alpha,\beta,p}$: expliciter α et β en fonction de a et b.*
2. *On suppose $p = 43, a = 5, b = 37$; on reçoit le message $E(x) = 28$. Que valait x ?*
3. *On a supposé p premier. Cette condition est-elle nécessaire pour avoir un chiffrement, c'est à dire pour que $D(E(x)) = x$?*
4. *On suppose que l'on connaît a, b et p. Soit M un message de n bits avec $n \gg \log_2 p$. Expliquer comment crypter M avec E et donner une estimation du temps nécessaire au cryptage de M avec E en fonction de n et p.*
5. *On désire maintenant utiliser les fonctions précédentes dans un système à clef privée, en supposant que p est connu : a, b et α, β sont privés, connus par Alice et Bob seulement.*
   Un espion sait qu'Alice envoie en secret à Bob les 2 messages différents x_1 et x_2, avec $0 \leq x_1, x_2 < p$. L'espion voit donc passer sur le réseau $y_1 = a.x_1 + b \mod p$ et $y_2 = a.x_2 + b \mod p$ (attaque par texte clair connu).
   Connaissant (x_1, y_1) et (x_2, y_2), montrer que l'espion peut alors facilement casser le code.
6. *On suppose maintenant que l'espion connait mais ne connait pas de couple clair-chiffré. Par contre il sait qu'Alice envoie à Bob un texte en français avec l'alphabet {'A', ..., 'Z', ' ', ',', '.'} de cardinal $p = 29$. Comment pouvez-vous casser ce chiffrement affine ?*

Exercice 3 (Mode de chaînage) *Etant donner une fonction de chiffrement (symétrique ou asymétrique) E_k associée à la fonction de déchiffrement D_k, pour éviter de chiffrer un bloc clair m par le même chiffré $c = E_k(m)$, on utilise des* modes de chiffrement*. Un mode de chiffrement est initailisé en entrée avec une valeur initiale (IV), constitué de bits aléatoires (et éventuellement d'information comme la date par exemple). En particulier, les modes suivants sont très utilisés. Grâce à ces modes de chiffrement, un même bloc clair n'est pas chiffré de la même façon si il est dans deux blocs différents. Par exemple, avec CBC, on déchiffre en calculant $m_i = c_{i-1} \oplus D_k(c_i)$.*

Question. *Un message M est découpé en n blocs $M = M_1, \ldots, M_n$ qui sont cryptés dans un schéma par blocs en $C = C_1, \ldots C_n$. Bob reçoit les blocs C_i, mais malheureusement, il ne sait pas qu'un et un seul des blocs a été transmis incorrectement (par exemple, des 1 ont été changés en 0 et vice versa durant la transmission du bloc C_1).*
Montrer que le nombre de blocs du message mal décryptés par Bob est égal à 1 si l'un des modes ECB, OFB ou CTR a été utilisé et égal à 2 si CBC ou CFB a été utilisé.

$$c_i = E_k(m_i \oplus c_{i-1}) \tag{1}$$

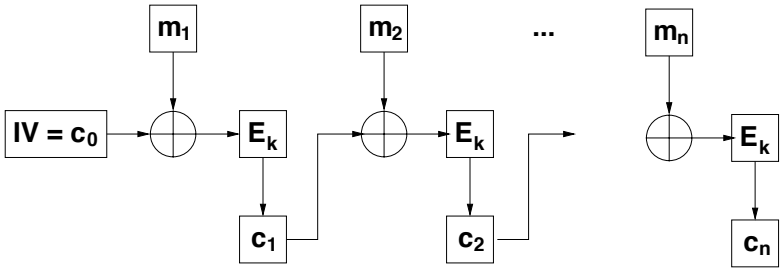

FIG. 1 – Mode de chiffrement par blocs CBC (Cipher Block Chaining).

$$z_0 = c_0 \ ; \ z_i = E_k(z_{i-1}) \ ; \ c_i = m_i \oplus z_i \tag{2}$$

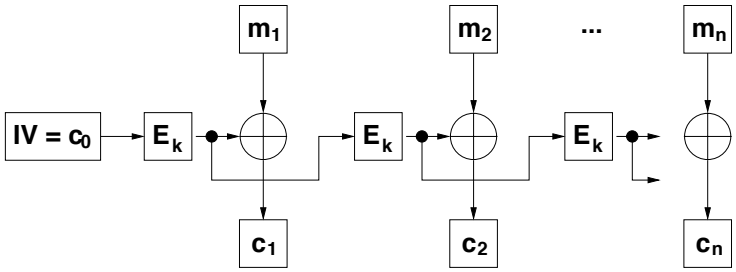

FIG. 2 – Mode de chiffrement par blocs OFB (Output FeedBack).

$$c_i = m_i \oplus E_k(T + i) \tag{3}$$

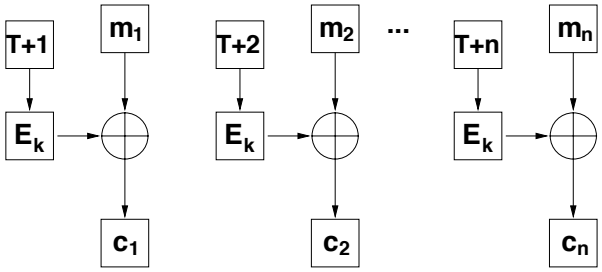

FIG. 3 – Le mode de chiffrement par blocs CTR (Counter) utilise un compteur de valeur initiale T.